Toolkit Template
Cyber Security State

Objective: This template has been developed to record critical basic information related to all aspects of your cyber security state and protections. The cyber landscape changes rapidly. This document provides guidance for protection from the risks current as the time of publication.

Cyber security is an essential factor in running and protecting any business. This toolkit provides general guidance for protecting your business.

- Who is the Anti-malware vendor?
    - Any they considered a leader in the field
- Does it cover more than viruses? Viruses are only one type of malware and your vendor needs to provide protection from a broader range of risks including but not limited to:
    - Viruses
    - Adware
    - Trojans
    - Ransomware
    - Web site corruptions
    - Phishing
    - Business email compromise
    - Other forms of malware
- Is the contract up to date?
    - Malware changes on a frequent basis and having a current contract for software updates is essential to protection
- Are updates installed automatically or tested first?
    - In most cases they should be done automatically unless there is some special software or condition that necessitates testing first
- Can a user stop or cancel the update?
    - Giving users the option to stop or cancel isn't advisable because they will lose valuable protection
- Is there a cyber education program in place?
    - Research shows people are the weakest link in cyber security
    - An education program is necessary to ensure people at all levels from the Board on down understand their role in protecting company assets including data
    - The program should be formal with periodic refreshers

  - All testing should conclude with testing to see if the material was learned
  - Surprise testing should be conducted periodically while employees are working and without announcement to see who succumbs to traps
- Is there a cyber policy and procedure in place?
  - This tells employees what to do and how to do it.
  - And what not to do
- Are all employees, without exception, required to take the training?
  - All employees regardless of level from the board on down need to take it and sign off that they have taken the training
  - Tests need to be given and the scores recorded
  - This is required for a cyber insurance claim to be paid
- What is the policy regarding use of company assets for personal use, such as accessing personal email or doing on-line shopping or going to non-business websites?
  - These actions are common but carry risk
  - A policy needs to be in place regarding this to protect the business and for a cyber insurance claim to be paid
- Is Bring Your Own Device, BYOD, permitted?
  - This is common today but does carry risk and all need to understand it
- If BYOD is permitted, what is the policy on the use of the device and ownership of the data?
  - It needs to be clearly spelled out
  - If the employee has personal data and company data on the device, how is ownership differentiated?
- Can the device be remotely wiped in case of loss or theft?
  - Wiping a device remotely is a good form of protection but employees need to understand that their personal data, photos and music will also be wiped
  - Has each employee signed the policy clearly stating that the firm can wipe the device including personal information, music and photos?
- Do employees work remotely such as from home?
- Is company issued equipment provided for this or are personal systems allowed to access company sites?
  - A policy must be in place regarding all these issues
- Is access permission for different software packages and systems granted on a need only basis or do all employees have access to all systems?
  - It’s common to provide access to everything to make sure people can get to what they need.
  - But it also provides much risk because if someone’s id is compromised it provides access to all company systems and information

- Providing access on a need only basis is preferred
- Role-based access models have been proven as provide needed access and also protect systems and information